Forsvarsministeriet Januar 2014

U D K A S T

Evaluering af GovCERT-loven

1. Indledning og sammenfatning

Forsvarsministeren afgiver hermed redegørelse om den statslige varslingstjeneste for internettrusler (GovCERT) og dens virksomhed efter § 9 i lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. (fremsat den 27. april 2011 som L 197).

Det er i loven fastsat, at ministeren senest tre år efter lovens ikrafttræden skal give Folketinget en skriftlig redegørelse på baggrund af en evaluering af den statslige varslingstjeneste for internettrusler (GovCERT) og dens virksomhed. Loven trådte i kraft den 1. juli 2011.

Evalueringen er nu foretaget. Det er den overordnede vurdering, at navnlig etableringen af Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste og placeringen af GovCERT som en del af centeret medfører behov for en ændring af retsgrundlaget for GovCERT's virksomhed. Dette sker ved fremsættelsen af forslag til en ny lov om Center for Cybersikkerhed. Et udkast til lovforslaget er sendt i høring samtidig med dette udkast til redegørelse.

Forsvarsministeriets konklusion på evalueringen er, at etableringen af GovCERT var velbegrundet, og at GovCERT's virksomhed har bidraget væsentligt til cybersikkerheden i Danmark. GovCERT bør således videreføres.

Imidlertid er der elementer i lovgrundlaget for GovCERT's virksomhed, som ikke er formålstjenlige. En revision af lovgrundlaget vurderes derfor at være af betydning for GovCERT's fremtidige virke som national, civil CERT og for GovCERT's evne til at bidrage til sikringen mod væsentlige angreb mod danske interesser.

Redegørelsen er en sammenfatning af de erfaringer, der er indhøstet, og de problemstillinger, som er konstateret, i den periode, GovCERT-loven har været i kraft. Da redegørelsen afgives i forbindelse med fremsættelsen af forslag til lov om Center for Cybersikkerhed, indeholder redegørelsen ikke konkrete anbefalinger til ændringer af lovgivningen. Der henvises i den forbindelse til lovforslaget.

Teknisk ekspertise fra Center for Cybersikkerhed samt tilbagemeldinger fra GovCERT's kunder i tidsrummet fra GovCERT's etablering i 2009 til dato er inddraget i evalueringen.

Der er i september 2013 nedsat et tilsyn med GovCERT, jf. lovens § 7. Tilsynet har endnu ikke afgivet sin første beretning, og der har derfor ikke kunnet indgå erfaringer herfra i evalueringen.

2. GovCERT's relevans

I tiden siden GovCERT's etablering har der såvel nationalt som internationalt været stigende opmærksomhed på cybertruslen. Danske offentlige myndigheder, virksomheder og privatpersoner er dagligt udsat for forstyrrende eller skadelige aktiviteter på internettet fra forskellige aktører. Der er også i 2013 set cyberangreb mod mål i Danmark, som i perioder har hindret anvendelse af dansk it-infrastruktur. Der er endvidere i de seneste år set cyberangreb mod væsentlige mål i Danmark, herunder Erhvervs- og Vækstministeriet og CSC, hvor informationssikkerheden er blevet kompromitteret.

I udlandet ser man samme udvikling. Den stigende opmærksomhed på cybertruslen har i de senere år medført etablering af nye nationale CERT'er (netsikkerhedstjenester) eller styrkelse af de eksisterende, ligesom der både i NATO og i EU er stærkt øget fokus på cybersikkerhedsområdet.

I forbindelse med etableringen af GovCERT udbyggedes Danmarks samarbejde med en række tilsvarende tjenester og internationale sikkerhedsfora betydeligt. GovCERT har derfor hurtigt kunnet virke som et betroet kontaktpunkt for udenlandske samarbejdspartnere. Dette har i flere tilfælde betydet, at GovCERT har modtaget information om observationer, hvor efterfølgende undersøgelser har ført til, at cyberangreb mod danske interesser er blevet opdaget. GovCERT's placering i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste har som forventet medført en yderligere styrkelse af det betroede samarbejde med internationale partnere.

På samme måde er GovCERT blevet et vigtigt kontaktpunkt for danske myndigheder og virksomheder i tilfælde, hvor de pågældende organisationer har haft mistanke om uregelmæssigheder. GovCERT har i en række tilfælde – i samarbejde med den pågældende myndighed eller virksomhed – kunnet konstatere forhold, som giver GovCERT en viden, der styrker GovCERT's mulighed for at beskytte de tilsluttede kunder.

På den baggrund kan det overordnet konkluderes, at etableringen af en statslig varslingstjeneste for internettrusler var velbegrundet.

3. GovCERT's konkrete bidrag til cybersikkerheden

Center for Cybersikkerhed, hvori GovCERT i dag indgår, har i flere tilfælde bistået med at imødegå målrettede cyberangreb. Blandt de eksempler, som har været beskrevet i pressen og dermed er offentligt kendte, kan nævnes kompromitteringen af Erhvervs- og Vækstministeriets systemer (herunder systemer placeret hos Statens It) i 2012 og sagen om kompromittering af CSC's systemer, hvor blandt andet Kørekortregistret og Schengen-registre anses for at være blevet kompromitteret.

GovCERT har i en række tilfælde kunnet yde et væsentligt bidrag til myndighedernes afdækning af omfanget af en uautoriseret indtrængen i myndighedens systemer og til at genvinde fuld kontrol med de angrebne systemer.

GovCERT's monitorering af internettrafikken ved hjælp af alarmenheder hos de tilsluttede kunder har til formål at tegne et normalbillede af netværkskommunikationen og dermed opnå det overblik, der er nødvendigt for at opdage eller vurdere afvigelser. Samtidig kan GovCERT hermed opnå et grundlag for at vurdere, om der bør udsendes varsling til GovCERT's kunder om et muligt angrebs karakter med rådgivning om modforholdsregler.

GovCERT kan konstatere cyberangreb og identificere relevante tekniske karakteristika herved ad flere veje. Det kan ske på baggrund af alarmer fra de tilsluttede alarmenheder, på baggrund af oplysninger fra samarbejdspartnere eller ud fra undersøgelser af mulige angreb, som er opdaget ad anden vej. Ved en opdatering af alarmenhederne hos de tilsluttede myndigheder og virksomheder kan GovCERT sikre, at lignende angreb mod andre kunder opdages.

GovCERT's adgang til at analysere den trafik, som passerer alarmenhederne, muliggør en vurdering af, om der i trafikken er karakteristika, der kan forbindes med angrebsformer, som i dag er udbredte. Der kan f.eks. være tale om indhold af tilforladeligt udseende i f.eks. Word- eller PDF-format, hvor alarmenhederne ved hjælp af analyseresultaterne kan opdage tegn på malware. Ligeledes har konsekvenserne af sikkerhedshændelser hos tilsluttede kunder kunnet klarlægges, herunder hvilke data m.v. en indtrængende hacker har kunnet foranstalte kopieret og videresendt ud af myndigheden.

GovCERT-lovens særlige adgang til monitorering af de tilsluttede kunders internettrafik har givet GovCERT mulighed for i samarbejde med den berørte myndighed at fastslå skadens omfang og beslutte relevante modforholdsregler, hvilket har understøttet en løbende styrkelse af cybersikkerheden i Danmark.

4. Tilslutning til GovCERT

Der har ikke været nogen tilslutningspligt til GovCERT. GovCERT har imidlertid i sin levetid opnået en meget høj tilslutningsgrad på det statslige område. Herudover er der sket tilslutning af flere kommuner og regioner samt virksomheder beskæftiget med kritisk infrastruktur.

16 ud af 19 mulige ministerområder er tilsluttet. Der arbejdes yderligere med tilslutning af Ministeriet for Fødevarer, Landbrug og Fiskeri samt Ministeriet for Sundhed og Forebyggelse, mens Ministeriet for Ligestilling og Kirke ikke har ønsket tilslutning.

Der er dog fortsat dele af de enkelte ministerområders it-infrastruktur, som i praksis ikke er dækket af GovCERT's alarmenheder. De enkelte ministerier har efter samråd med GovCERT indikeret, hvor tilslutning til GovCERT ville have størst sikkerhedsmæssig effekt. Samtidig har GovCERT efter aftale med de berørte ministerier og Statens It tilsluttet væsentlige dele af Statens It, som leverer it-drift til en række ministerområder.

En oversigt over tilsluttede myndigheder og virksomheder er medtaget som bilag.

Den høje tilslutningsgrad i staten i løbet af meget kort tid må i lyset af erfaringer fra tilsvarende tjenester i udlandet karakteriseres som en betydelig succes.

5. GovCERT's dækningsområde

GovCERT oprettedes – som det er anført i de almindelige bemærkninger til lovforslaget, pkt. 1.2.1 – bl.a. for "at mindske risikoen for it-angreb, herunder at offentlige myndigheders elektroniske kommunikation med omverdenen bliver afskåret i flere dage, eller at dokumenter uden myndighedens vidende bliver sendt til fremmede stater som følge af et virusangreb. Dette kan udgøre en sik-

kerhedsrisiko og også have store administrative og økonomiske konsekvenser til følge. Tilsvarende gør sig gældende for private virksomheder beskæftiget med kritisk infrastruktur."

GovCERT blev etableret som en statslig varslingstjeneste. Der blev i årene 2009-2012 gennemført pilotforsøg med en udvidelse af GovCERT's dækningsområde til at omfatte kommuner og virksomheder beskæftiget med kritisk infrastruktur.

Det har vist sig, at der fra flere sider er forventninger til, at GovCERT's nationale overblik over trusler og sårbarheder i tjenester, net og systemer relateret til internettet kunne komme en bredere kreds til gode. Der er fra brancheside udtrykt ønske om, at en offentlig CERT-funktion skulle kunne dække flere private virksomheder.

I tiden siden fremsættelsen af forslaget til GovCERT-loven i foråret 2011 er der såvel nationalt som internationalt sket en ændring i synet på cybertruslen. Hvor man for bare få år siden fokuserede på truslen ved hacking, overbelastningsangreb og botnet-malware, er der nu stigende opmærksomhed på truslen fra såkaldte APT-angreb (Advanced Persistent Threats) og malware distribueret med spionagehensigt. Disse trusler er sværere at identificere, og angreb vil typisk være længerevarende og svære at opdage uden meget specifikke oplysninger om, hvad de it-sikkerhedsansvarlige skal kigge efter.

Der er hermed i et vist omfang sket en forskydning i opfattelsen, fra at cyberangreb væsentligst var en trussel imod tilgængeligheden, til at cyberangreb i væsentlig grad truer fortroligheden.

En række danske virksomheder af væsentlig betydning for forskning og videnskabelse i Danmark og dansk eksport, herunder forsvars- og aerospaceindustrien, leverer ydelser eller bidrager på anden vis væsentligt til opretholdelsen af sikkerheden i samfundet (herunder den nationale sikkerhed i et vækst- og velfærdsperspektiv). Da de typisk ikke kan karakteriseres som værende beskæftiget med kritisk infrastruktur, falder de uden for lovens definition af GovCERT's dækningsområde (ud over staten er kommuner og regioner samt private virksomheder, som er beskæftiget med kritisk infrastruktur, omfattet, jf. lovens § 2, stk. 1).

Det er endvidere set, at f.eks. en virksomhed, som ikke er omfattet af GovCERT's aktuelle dækningsområde, og som ikke kan anses for at være af væsentlig samfundsmæssig betydning i sig selv, har været udsat for et cyberangreb med en kompromittering af væsentlig samfundsmæssig betydning. I de tilfælde har den pågældende virksomhed potentielt kunnet anvendes som mulig angrebsplatform mod væsentlige danske interesser. Ved mistanke om sådanne angreb ville det tjene GovCERT's formål, såfremt der kunne gennemføres en midlertidig tilslutning til GovCERT af den angrebne virksomhed.

Det har generelt vist sig, at værdien ved en tilslutning til GovCERT – både for den enkelte myndighed eller virksomhed og for bidraget til et højt informationssikkerhedsniveau i samfundet – afhænger af, at den pågældende myndighed eller virksomhed har et tilfredsstillende informationssikkerhedsniveau og en it-driftsorganisationen med et beredskab, der kan håndtere information fra GovCERT. En sådan modenhed bør derfor også være et relevant tilslutningskriterium.

Dækningsområdet for GovCERT som den nationale, civile CERT bør således udvides.

6. Regler for sletning af data

I lovens § 4 er fastsat frister for sletning af data. Pakkedata (indholdet af internetbaseret kommunikation) kan i den forbindelse højst opbevares 14 dage, hvorefter data skal slettes. Trafikdata (data, som behandles med henblik på overførsel af pakkedata) kan højst opbevares i 12 måneder.

Lovens sletningskrav forhindrer i praksis bl.a. GovCERT i at fastlægge et normalbillede af en kundes internettrafik, som tager højde for en kundes regelmæssigt afvigende trafikmønstre (f.eks. ved en månedlig backup-procedure eller en årlig regnskabsaflæggelse). Et utilstrækkeligt normalbillede vanskeliggør identifikationen af en indtrængende parts uautoriserede aktiviteter såsom kopiering af større mængder data, anvendelse af systemer på usædvanlige tidspunkter m.v.

I de tilfælde, hvor GovCERT har opdaget angreb på baggrund af oplysninger fra samarbejdspartnere eller ad anden vej, har det i praksis vist sig, at angrebet først opdages mere end 14 dage efter, at det har fundet sted. Det vanskeliggør identifikation og imødegåelse af angrebet og reducerer muligheden for at opsamle viden om angrebets karakteristika, at pakkedata på det tidspunkt ikke længere er til rådighed.

Det havde også været hensigtsmæssigt, hvis GovCERT, når en konkret myndighed eller virksomhed er blevet ramt af et cyberangreb, kunne undersøge, om andre tilsluttede myndigheder og virksomheder er eller har været ramt af tilsvarende angreb. En sådan undersøgelse kan i sagens natur først indledes, når der er konstateret et angreb, og GovCERT har kortlagt eller modtaget oplysninger om et givet angrebs egenskaber – såsom angrebsmetoder og anvendte IP-adresser. Det ville være formålstjenligt i forhold til GovCERT's formål, såfremt det ved gennemgang af historiske trafik- og pakkedata kunne undersøges, om der er tegn på tilsvarende aktivitet hos tilsluttede myndigheder og virksomheder.

Det kan samlet konstateres, at længere frister for opbevaring af historiske data ville være af betydelig sikkerhedsmæssig værdi.

7. Regler for videregivelse af data

GovCERT's varslinger til kunder indeholder, når det er relevant, oplysninger om karakteristika ved en konstateret type angreb eller trussel herom, herunder f.eks. IP-numre, som vurderes at have forbindelse til angriberen. Dette giver kunderne bedre forudsætninger for at gennemse egne systemer for tegn på sådanne angreb og at øge beskyttelsen selv (i egne firewalls m.v.). De pågældende karakteristika kan være identificeret ved analyser af trafikdata fra GovCERT's alarmenheder.

Efter GovCERT-loven har GovCERT imidlertid ikke mulighed for at videregive denne type oplysninger til danske televirksomheder og internetudbydere (såkaldte udbydere af offentlige elektroniske kommunikationsnet og -tjenester). Sådanne virksomheders sikkerhedssystemer spiller imidlertid en central rolle for sikkerheden i den danske kommunikationsinfrastruktur. Denne sikkerhed ville være højnet, såfremt GovCERT havde haft adgang til at videregive denne type oplysninger til udbyderne.

Visse af begrænsningerne på GovCERT's videregivelse af oplysninger i forbindelse med varslinger besværliggør således i konkrete tilfælde sikringen mod væsentlige angreb mod danske interesser, uden at begrænsningen i de konkrete tilfælde synes formålstjenlig i øvrigt.

Det kan samlet konstateres, at der er behov for en revurdering af reglerne for videregivelse af data.

8. Ny organisation på it-sikkerhedsområdet

Siden kongelig resolution af 3. oktober 2011 har GovCERT hørt under Forsvarsministeriets ressort. Af regeringsgrundlaget af samme dato fremgår, at "For at styrke beskyttelsen mod cyberangreb mv. samles de forskellige myndigheders indsats i et IT sikkerhedscenter (under Forsvarsministeriet), der skal varetage opgaven som den nationale IT-sikkerhedsmyndighed og Governmental Computer Emergency Response Team (GovCERT)."

På den baggrund blev Center for Cybersikkerhed oprettet den 18. december 2012 som en del af Forsvarets Efterretningstjeneste. Center for Cybersikkerhed omfatter ud over GovCERT bl.a. MIL-CERT, der er varslingstjeneste for internettrusler på Forsvarsministeriets område.

Den nye organisation har betydet, at GovCERT i kraft af sin placering i FE har fået adgang til flere oplysninger fra betroede internationale partnere om cybertrusler. En række af disse oplysninger har kunnet omsættes i en styrkelse af sikkerheden for GovCERT's kunder.

GovCERT's placering under FE betyder imidlertid også, at GovCERT's virksomhed ikke længere er omfattet af persondataloven. Dette har betydet bortfaldet af en væsentlig forudsætning for Gov-CERT-lovens regulering af GovCERT's virksomhed. Forsvarsministeren har bl.a. derfor udstedt retningslinjer for Center for Cybersikkerhed, som stiller krav om efterlevelse af relevante principper i persondataloven.

Der er endvidere med ressortændringen sket en væsentlig ændring i grundlaget for det efter Gov-CERT-loven etablerede tilsyn, ikke mindst i lyset af det Tilsyn med Efterretningstjenesterne, som er etableret efter FE-loven og PET-loven.

Der er således behov for at tilpasse lovgrundlaget til den nye organisation på it-sikkerhedsområdet.

Bilag A. Oversigt over tilsluttede myndigheder og virksomheder

Der er aktuelt indgået tilslutningsaftaler på følgende ministerområder*:

- Beskæftigelsesministeriets område
- Erhvervs- og Vækstministeriets område
- Finansministeriets område
- Justitsministeriets område
- Klima-, Energi- og Bygningsministeriets område
- Kulturministeriets område
- Miljøministeriets område
- Ministeriet for By, Bolig og Landdistrikters område
- Ministeriet for Forskning, Innovation og Videregående Uddannelsers område
- Ministeriet for Sundhed og Forebyggelses område
- Skatteministeriets område
- Social-, Børne- og Integrationsministeriets område

- Statsministeriets område
- Transportministeriets område
- Udenrigsministeriets område
- Undervisningsministeriets område
- Økonomi- og Indenrigsministeriets område

Øvrige myndigheder og virksomheder, der aktuelt er indgået tilslutningsaftale med:

- Region Hovedstaden
- Hillerød Kommune
- Odense Kommune
- DONG
- KMD
- TDC

Ministerområder under tilslutning:

- Ministeriet for Fødevarer, Landbrug og Fiskeris område

Myndigheder og virksomheder tilsluttet i forbindelse med forsøget med en udvidelse af GovCERT's dækningsområde, men som ikke længere er tilsluttet:

- Viborg Kommune

*) MILCERT er varslingstjeneste på Forsvarsministeriets område. GovCERT og MILCERT er i dag samlet i Center for Cybersikkerhed, og monitoreringen af centerets egen netværkstrafik varetages af GovCERT.

Bilag B. GovCERT's varslinger om hændelser

GovCERT har i perioden september 2011 til udgangen af 2013 udsendt godt 100 varslinger til GovCERT's kundekreds. Tallet omfatter generelle varslinger til en bredere kreds og specifikke varslinger til enkeltkunder på baggrund af en alarm.

Der er siden 2010 registreret lidt over 1.000 sikkerhedshændelser. Heraf vurderes en fjerdedel at være alvorlige.

Blandt de alvorlige hændelser er overbelastningsangreb og APT-angreb. Mindre alvorlige hændelser omfatter fund af tegn på infektion med vira og forskellige typer malware (crimeware, botnet-malware mv.).